

Video Forgery Detection using Machine Learning

Gaikwad Kanchan¹, Kandalkar Ambika², Khokale Yogita³, Bhagwat Archana⁴,
Chandgude Amar⁵

^{1,2,3,4}Student, Dept. of Computer Engineering, S.N.D. college of Engineering and Research Center Yeola,
Maharashtra, India

⁵Professor, Dept. of Computer Engineering, S.N.D. college of Engineering and Research Center Yeola,
Maharashtra, India

Abstract – Video and image copy-move forgery detection is one of the major topic in multimedia forensics to protect digital videos and images from malicious use. Number of approaches have been presented through analyzing the side effect caused by copy-move operation. However, based on multiple features similarity calculations or unstable image features, a few can well balance the detection efficiency, robustness, and applicability. In this paper, we propose a novel approach to detect frame copy-move forgery. And also coarse-to-fine detection strategy based on optical flow (OF) and stable parameters is designed to detect. Specifically, coarse detection analyzes OF sum consistency to find suspected tampered points. Fine detection is then conducted for precise location of forgery, including duplicated frame pairs matching based on OF correlation and validation checks to further reduce the false detections. This system uses the GLCM for feature extraction and SVM will be used for classification and ANN is used to train the dataset.

Key Words- OPTICAL FLOW(OF); ARTIFICIAL NEURAL NETWORKS; GLCM FEATURE; GUI; MACHINE LEARNING; SUPPORT VECTOR MACHINE.

1. INTRODUCTION

There is a significant role of digital images in our daily life. However, image manipulation has become very easy by using powerful software. Documents or images can be scanned using this software and manipulated without any doubt. Image authenticity now is a big concern. Image forgeries may be classified into many types- such as copy-move forgery, splicing and many more. Two main types of image forensic techniques are to verify the integrity and authenticity of manipulated image. One is active forensic method and another is passive forensic method. In active methods Watermarking and steganography are two techniques which are used to insert authentic information into the image. In the authenticity of an image, then prior embedded authentication information is recalled to prove the authenticity of that image. However, embedding authentication of information to an image is very reliable. Only an authorized individual allows to do it or at the time of creating the image, authentic information could be embedded as well. But requirement of special cameras and multiple steps processing of the digital image are two main limitations which made this technique less popular. To avoid these limitations, passive forensic technique are utilize

image forgery without requiring detailed previous Information. The most widely used method to construct forged image is copy-move forgery. It refers to copy one part from image, and paste it inside the same image. Sometime before pasting the copied regions, various post-processing operations like scale, rotation, blurring, intensifying or JPEG compression may be applied.

2. LITERATURE SURVEY

A. Block-based Image Forgery Detection

In block-based method, input image size of $M \times N$ is segmented into overlapping blocks size of $z \times z$ resulting into overlapping blocks, $L = (M-z+1) \times (N-z+1)$. A few features are extricated from each block. Distinctive features are extracted by applying different feature extraction technique such as DCT (Discrete Cosine Transform) [9], DWT (Discrete Wavelet Transform) [10], DFT(Discrete Fourier Transform) [10], PCA (Principal Component Analysis) [12] [13], SVD (Singular Value Decomposition) [14][15], and ZMs (Zernike Moments) [16]. Then, a comparison is done based on blocks features similarity and distance. After finding the most matched or similar features blocks, copy-move region is identified and this region is localized. Sheng et al. [9] proposed forgery detection algorithm using block-based method. This algorithm uses DCT and circle blocking technique for extracting features of the image. Finally, the image which contains singularities within lines is presented by computing ridgelet transformation. Robustness against JPEG compression is the most significant feature of this method.

Cao et al. [17] followed block-based method to detect tampered region where DCT feature extraction technique is applied. DCT is applied to divide sub blocks to extract key features by producing quantized coefficients. Threshold value are set prior to match features between closest similar image blocks. This method shows less computational complexity compared to existing methods [23-[18] because of reducing dimension of feature vector. Later, similar method and feature extraction technique used by Huang et al. [19]. The big difference in the result with Cao et al.'s DCT-based method [17], because of reducing the false matches rate. Due to low false matches rate, this method becomes powerful against noise and blurring. However, it is not robust for rotation attack and cannot detect multiple forgery.

M. Bashar et al.,[20] developed more efficient forgery detection method based on DWT and kernel PCA (KPCA) features. Natural images have been used as a dataset in this method. As a consequence of quantitative analysis considering noiseless and uncompressed factor, it is found that the DWT performs well than KPCA in terms of features. On the other hand, in noise and JPEG compression domain, KPCA-based features perform better than DWT. The method shows robustness against noise and JPEG compression attack. Though the method takes too much time and not robust against scaling. It cannot detect multiple forgery.

B. Key point-based Image Forgery Detection Method

Different from block-based methods, features are extracted in key points-based method from the image without any type segmentation. Extracted features from every key points are compared to find similarities between them. Finally, based on the calculation of matched features, image forgery is detected. SIFT and SURF (Speeded Up Robust Features) are two main key points based feature extraction methods. Somayeh Sadeghi et al., [21] and Diao M. uliyan et al., [22] worked on key points based technique (e.g. SIFT). Sadeghi et al., proposed SIFT to extract features and searched for similar features based on their Euclidean distance. Both methods are robust against several post-processing attacks; including scale, noise, rotation and JPEG compression. However, inability to detect small forged areas and performance of detection and localization for those forged areas are also questionable. In [22], primary approach of Uliyan et al., was to detect image regions by using Statistical Region Merging (SRM) Segmentation algorithm. Then, the experiment proceeded with applying Angular Radial Partitioning (ARP) and Harris Corner detection method on the image region. Finally, forged regions were detected based on matched key points. The method showed less robustness against forged regions with blurring and illumination attacks. Moreover, it shows different result for same image with different resolution. The major drawbacks of the previously mentioned conventional techniques are either not powerful against all post processing attacks or have high computation time. Therefore, keeping up the low computational time is the most important robustness challenge. To tackle this issue, a new copy-move forgery detection method is proposed where region wise image segmentation is done. Gabor filters are used to extract image features. Afterwards, K Means clustering, and Euclidean distance calculation facilitated to detect forged region from the suspicious image. Reducing the false matching rate is the most significant task to exhibit the proposed method as more viable compared to conventional methods.

3. PROPOSED SYSTEM

A. Video Input:

Video forensic has become an important area of research in the last decade. System will accept video as an input.

Justified format of video should be given as an input to get processed.

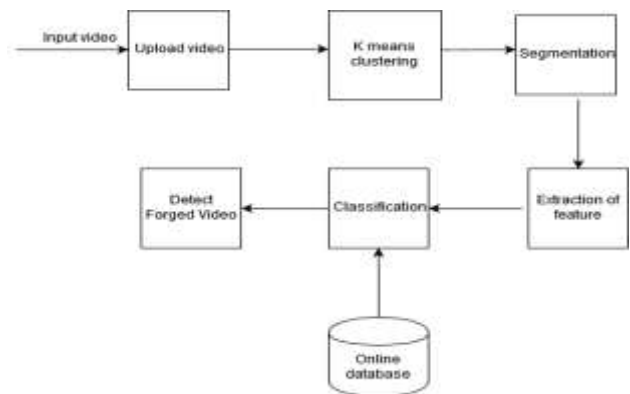


FIG 1: BLOCK DIAGRAM

B. Video Parsing/Segmentation:

Input video is been accepted and done parsing based on fps. These frames will be temporary stored in backend for further processing and feature extraction.

C. K-Means Clustering

K-means clustering is a technique for quantizing vectors. This method divides the image into k segments, each containing mutually exclave data. This is a common method when it comes to pattern recognition and machine learning. One of the segmented images is chosen on the basis of the information contained in it. To determine this, the features of each segment are calculated and the segment with the highest mean is chosen. The features of the segmented image are then compared with the original image using cross-validation, which gives another array, which is studied to determine whether an image is morphed or not, and function for the final result is added on the basis of that.

D. Feature Extraction:

Extraction of Features: Out of all the methods to analyze an image, extraction of GLCM features has proven to be efficient time and time again. The gray level co-variance matrix is a tabulation that provides with statistical measures for texture analysis. This method takes into account the spatial relationship between the intensities of pixels in a gray-level image. In this paper, the GLCM features were calculated to study the differences in the original image and the digitally forged image. This gave 22 texture values (for each image) to work with, most of which were similar when it came to an image and its fraudulent counterpart. In practice, this would lead to redundancy and would also increase the time to run the algorithm. Also, the histogram of oriented gradient (HOG) features was calculated which gave another set of features for the original and the morphed image. The HOG values of the original and the morphed images were reasonably apart from each other, which meant that these values will be useful in differentiating the original document from the morphed one. However, the order of matrix

generated by HOG algorithm is too large to be successfully fed into an SVM so it could also not be of practical use.

E. Online Database

Also, the Features values were computed but since the order of the matrix produced were very large to be trained by using ANN machine learning algorithm so as to enhance accuracy.

F. Classification

Initially, the classifier used for classification of dataset into two parts as original or morphed was linear kernel SVM. A linear kernel SVM is the most suitable classifier for two-class classification problems. It finds an equivalent hyperplane which separates the whole data by a specific criterion that depends on the algorithm applied. It tries to find out a hyperplane which is far from the closest samples on the other side of the hyper plane while still classifying samples. It gives the best generalization techniques because of the larger margin.

G. Detection of the Forged region

After the identification of duplicate blocks, the further step is to highlight the duplicate blocks on the digital image, which also gives an indication of forged regions. Hence, system finally detects forged areas in the digital image. The corresponding forged regions are being highlighted by the system.

4. PROPOSED ALGORITHM:

- i. The standard database consists of original, forged and processed images is considered in the performance analysis.
- ii. The images in the database are converted to gray scale.
- iii. The statistical features are computed on GLCMs which is developed from the gray scale images.
- iv. The Support Vector Machine(SVM) is trained with statistical features for every image in the database using RBF kernel.
- v. Statistical features of the testing image are obtained in similar process using steps ii and iii.
- vi. Then the SVM classifier classifies the image either to be authenticated or forged one.

CONCLUSION

In this way, we are going to implement the system for image and video forgery detection using ANN feature. By using GLCM feature this will classify the frame into different cluster and by using SVM method this system will generate the output as the image is forged or not.

REFERENCES

- [1] Shruti Ranjan, Prayati Garhwal, Anupama Bhan, Monika Arora, Anu Mehra " Framework For Image Forgery Detection And Classification Using Machine Learning", IEEE Xplore Compliant Part Number: CFP18K74-ART; ISBN:978-1-5386-2842-3.
- [2] H M Shahriar Parvez, Hamid A. Jalab, and Somayeh Sadegh, "Copy-move Image Forgery Detection Based on Gabor Descriptors and K-Means Clustering" . (ICSCEE2018) ©2018 IEEE.
- [3] R. Poisel and S. Tjoa, "Forensics investigations of multimedia data: A review of the state-of-the-art," in Proceedings - 6th International Conference on IT Security Incident Management and IT Forensics, IMF 2011, 2011, pp. 48-61.
- [4] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, no. 3, pp. 226-245, 2013.
- [5] G. Lynch, F. Y. Shih, and H. Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," Inf. Sci. (Nij.), vol. 239, pp. 253-265, 2013.
- [6] H. C. Hsu and M. S. Wang, "Detection of copy-move forgery image using Gabor descriptor," in Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID, 2012.
- [7] D. M. Uliyan, H. A. Jalab, A. Abuarqoub, and M. Abu-Hashem, "Segmented-Based Region Duplication Forgery Detection Using MOD Keypoints and Texture Descriptor," in Proceedings of the International Conference on Future Networks and Distributed Systems, 2017, p. 6:1--6:6.
- [8] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3 PART 2, pp. 1099-1110, 2011.
- [9] G. Sheng, T. Gao, Y. Cao, L. Gao, and L. Fan, "Robust algorithm for detection of copy-move forgery in digital images based on ridgelet transform," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2012, vol. 7530 LNAI, pp. 317-323.
- [10] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digital Investigation, vol. 9, no. 1, pp. 49-57, 2012.
- [11] B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation," IEEE Trans. Inf. Forensics Secur., vol. 3, no. 3, pp. 529-538, 2008.

- [10] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Department of Computer Science., Dartmouth Coll. Tech. Rep. TR2004-515, no. 2000, pp. 1–11, 2004.
- [11] Z. Moghaddasi, H. A. Jalab, R. Md Noor, and S. Aghabozorgi, "Improving RLRN Image Splicing Detection with the Use of PCA and Kernel PCA," *Sci. World J.*, vol. 2014, 2014.
- [12] D. Y. Huang, T. W. Lin, W. C. Hu, and C. H. Chou, "Boosting scheme for detecting region duplication forgery in digital images," in *Advances in Intelligent Systems and Computing*, 2014, vol. 238, pp. 125–133.
- [13] W. Luo, Z. Qu, J. Huango, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2007, vol. 2.
- [14] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 8, pp. 1355–1370, 2013.
- [15] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," *Forensic Sci. Int.*, vol. 214, no. 1–3, pp. 33–43, 2012.
- [16] D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, P. Shivakumara, and S. Sadeghi, "A novel forged blurred region detection system for image forensic applications," *Expert System Application*, vol. 64, pp. 1–10, 2016.
- [17] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," *Forensic Sci. Int.*, vol. 206, no. 1–3, pp. 178–184, 2011.
- [18] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, "Exploring duplicated regions in natural images," *IEEE Trans. Image Process.*, no. 99, 2010.
- [19] S. Sadeghi, H. A. Jalab, K. S. Wong, D. Uliyan, and S. Dadkhah, "Key point based authentication and localization of copy-move forgery in digital image," *Malaysian J. Computer. Science.*, vol. 30, no. 2, pp. 117–133, 2017.
- [20] D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, and S. Sadeghi, "Image region duplication forgery detection based on angular radial partitioning and harris key-points," *Symmetry (Basel)*, vol. 8, no. 7, 2016.